



## PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

**CUALIFICACIÓN PROFESIONAL: GESTIÓN DE SISTEMAS INFORMÁTICOS**

**Código: IFC153\_3**

**NIVEL: 3**

### CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

#### UNIDAD DE COMPETENCIA

**“UC0486\_3: Asegurar equipos informáticos”**

#### LEA ATENTAMENTE LAS INSTRUCCIONES

Conteste a este cuestionario de **FORMA SINCERA**. La información recogida en él tiene **CARÁCTER RESERVADO**, al estar protegida por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Su resultado servirá solamente para ayudarle, **ORIENTÁNDOLE** en qué medida posee la competencia profesional de la “UC0486\_3: Asegurar equipos informáticos”

No se preocupe, con independencia del resultado de esta autoevaluación, Ud. **TIENE DERECHO A PARTICIPAR EN EL PROCEDIMIENTO DE EVALUACIÓN**, siempre que cumpla los requisitos de la convocatoria.

Nombre y apellidos del trabajador/a: NIF:	Firma:
Nombre y apellidos del asesor/a: NIF:	Firma:



### INSTRUCCIONES CUMPLIMENTACIÓN DEL CUESTIONARIO:

Las actividades profesionales aparecen ordenadas en bloques desde el número 1 en adelante. Cada uno de los bloques agrupa una serie de actividades más simples (subactividades) numeradas con 1.1., 1.2.... en adelante.

Lea atentamente la actividad profesional con que comienza cada bloque y a continuación las subactividades que agrupa. Marque con una cruz, en los cuadrados disponibles, el indicador de autoevaluación que considere más ajustado a su grado de dominio de cada una de ellas. Dichos indicadores son los siguientes:

1. No sé hacerlo.
2. Lo puedo hacer con ayuda
3. Lo puedo hacer sin necesitar ayuda
4. Lo puedo hacer sin necesitar ayuda, e incluso podría formar a otro trabajador o trabajadora.

<b>1. Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad.</b>	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1. Analizar el plan de implantación del sistema informático de la organización comprobando que incorpora: <ul style="list-style-type: none"><li>- Información referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones, entre otros.</li><li>- Referencias de posibilidades de utilización de los equipos y restricciones de los mismos.</li><li>- Protecciones contra agresiones de virus y otros elementos no deseados, entre otros.</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2. Asignar (provisionar) los permisos de acceso, por parte de los usuarios, a los distintos recursos del sistema por medio de las herramientas correspondientes según el Plan de Implantación y el de seguridad del sistema informático.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3. Garantizar la confidencialidad e integridad de la conexión en el acceso a servidores según las normas de seguridad de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.4. Analizar las políticas de usuario verificando que quedan reflejadas circunstancias tales como usos y restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



<b>1. Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad.</b>	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.5. Transmitir la política de seguridad a los usuarios, asegurándose de su correcta y completa comprensión.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.6. Documentar las tareas realizadas según los procedimientos de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.7. Tratar las informaciones afectadas por la normativa aplicable de protección de datos verificando que los usuarios autorizados cumplan los requisitos indicados por la normativa y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<b>2. Configurar servidores para protegerlos de accesos no deseados según las necesidades de uso y dentro de las directivas de la organización.</b>	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1. Ubicar el servidor en la red en una zona protegida y aislada según las normas de seguridad y el plan de implantación de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2. Activar y configurar los servicios que ofrece el servidor desactivando los innecesarios según la normativa aplicable de seguridad y plan de implantación de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3. Configurar los accesos y permisos a los recursos del servidor por parte de los usuarios en función del propósito del propio servidor y de la normativa de seguridad de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.4. Activar los mecanismos de registro de actividad e incidencias del sistema y habilitar los procedimientos de análisis de dichas informaciones, de forma que permitan sacar conclusiones a posteriori.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



<b>2. Configurar servidores para protegerlos de accesos no deseados según las necesidades de uso y dentro de las directivas de la organización.</b>	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.5. Decidir la utilización de los módulos adicionales del servidor en base a sus funcionalidades y riesgos de seguridad, llegando a una solución de compromiso.				
2.6. Configurar los mecanismos de autenticación para que ofrezcan niveles de seguridad e integridad en la conexión de usuarios de acuerdo con la normativa de seguridad de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.7. Definir y asignar los roles y privilegios de los usuarios siguiendo las instrucciones que figuren en las normas de seguridad y el plan de explotación de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<b>3. Instalar y configurar elementos de seguridad (cortafuegos, equipos trampa, Sistemas de Prevención de Intrusión o Firewalls, entre otros) en equipos y servidores para garantizar la seguridad ante los ataques externos según las necesidades de uso y dentro de las directivas de la organización.</b>	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1. Seleccionar la topología del cortafuegos en función del entorno de implantación.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2. Elegir los elementos hardware y software del cortafuegos teniendo en cuenta factores económicos y de rendimiento.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3. Instalar y configurar los cortafuegos según el nivel definido en la política de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.4. Determinar, configurar y administrar las reglas de filtrado y los niveles de registro y alarmas según las necesidades dictaminadas por la normativa de seguridad de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



<b>3. Instalar y configurar elementos de seguridad (cortafuegos, equipos trampa, Sistemas de Prevención de Intrusión o Firewalls, entre otros) en equipos y servidores para garantizar la seguridad ante los ataques externos según las necesidades de uso y dentro de las directivas de la organización.</b>	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.5. Verificar los cortafuegos con juegos de pruebas, asegurando que superan las especificaciones de la normativa de seguridad de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6. Documentar la instalación y actualización del cortafuegos y los procedimientos de actuación con el mismo según las especificaciones de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.7. Definir y configurar los sistemas de registro para la revisión y estudio de los posibles ataques, intrusiones y vulnerabilidades.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>